SUMMARY TABLE FOR: "Internet PKI, Operational Protocols - LDAPv2," draft-ietf-pkix-ipki2opp-07.txt, March 1998

28 May 1998

Prepared by:

Center for Standards
Defense Information Systems Agency

This supercedes version dated 7 May 1998 and all earlier versions.

This Page left intentionally blank.

Disclaimer

Persons and organizations use this document at their own risk.

This document is for information only. If there is any conflict between this document and the source document, the source document takes precedence.

The U. S. Federal Government does NOT provide any guarantee as to the accuracy of this document. This document is NOT a request for proposal, a request for bid, or a modification to any contract currently held with the U. S. Federal Government.

Distribution of this document is unlimited.

Acronyms

CA - Certification Authority
PSE - Personal Security Environment

This Page left intentionally blank.

STATUS CODES: M – MANDATORY, O – OPTIONAL, C - CONDITIONAL

SECTION	FEATURE	STATUS	REMARKS
5	**Lightweight Directory Access Protocol (LDAP)**	M	
	LDAPv2	M	ref. RFC1777, RFC1778
6	**LDAP Repository Read**	M	
6.1	**Bind**	M	ref. RFC1777:sec 4.1
6.1.1	**Bind Request**	M	
	Syntax	M	
	version INTEGER (2)	M	
	name LDAPDN	M	ref. RFC1779
	Accept NULL LDAPDN	M	
	simpleauth OCTET STRING	M	
	Accept NULL	M	
	Anonymous search access	O	RECOMMENDED
	Restrict search criteria	O	
	Authenticated search access	O	
	Implementation of other aspects of protocol element by application providing LDAP repository read service	O	
6.1.2	**Bind Response**	M	
	Implementation of entire protocol element by application providing LDAP repository read service	M	
	Minimum set of error codes recognized by clients	O	ref. RFC1777:sec. 4
	success (0)	M	
	operationsError (1)	M	
	protocolError (2)	M	
	authMethodNotSupported (7)	M	
	noSuchObject (32)	M	
	invalidDNSyntax (34)	M	
	inappropriateAuthentication (48)	M	
	invalidCredentials (49)	M	
	busy (51)	M	
	unavailable (52)	M	
	unwillingToPerform (53)	M	
	other (80)	M	
6.2	**Search**	M	ref. RFC1777:sec. 4.3
6.2.1	**Search Request**	M	base object search w/ a filter testing for objectClass attribute ref. RFC1777:sec. 4.3
	Syntax		
	baseObject LDAPDN	M	ref. RFC1779
	scope	M	
	baseObject LDAPDN	M	
	derefAliases	M	
	neverDerefAliases	M	do not dereference aliases in searching or in locating the base object of the search
	sizeLimit INTEGER (0)	M	
	timeLimit INTEGER (0)	M	
	attrsOnly BOOLEAN	M	
	FALSE	M	both attribute types and values returned

SECTION	FEATURE	STATUS	REMARKS
	filter	M	
	present AttributeType	M	ref X.500
	attributes AttributeType	M	ref X.500
	Implementation of other aspects of protocol element by application providing LDAP repository read service	O	
6.2.2	**Search Response**	M	ref. RFC1777:sec. 4.3
	Implementation of entire protocol element by application providing LDAP repository read service	M	
	Syntax		
	objectName LDAPDN	M	ref. RFC1779
	attributes	M	
	AttributeType	M	ref X.500
	SET of AttributeValue	M	ref. RFC1778
	All values of multivalued attributes are returned	M	assumes requester has sufficient access permissions
	resultCode LDAPResult	M	ref. RFC1777:sec. 4
6.3	**Unbind**	M	ref RFC1777:sec. 4.2
	Implementation of full UnbindRequest by application providing LDAP repository read service	M	
7	**LDAP Repository Search**	M	ref. RFC1777:sec. 4.1
7.1	**Bind**	M	ref. 6.1
	Bind Request	M	
	Syntax	M	
	version INTEGER (2)	M	
	name LDAPDN	M	ref. RFC1779
	Accept NULL LDAPDN	M	
	simpleauth OCTET STRING	M	
	Accept NULL	M	
	Anonymous search access	O	RECOMMENDED
	Restrict search criteria	O	
	Authenticated search access	O	
	Implementation of other aspects of protocol element by application providing LDAP repository search service	O	
	Bind Response	M	
	Implementation of entire protocol element by application providing LDAP repository read service	M	
	Minimum set of error codes recognized by clients	O	ref. RFC1777:sec. 4
	success (0)	M	
	operationsError (1)	M	
	protocolError (2)	M	
	authMethodNotSupported (7)	M	
	noSuchObject (32)	M	
	invalidDNSyntax (34)	M	
	inappropriateAuthentication (48)	M	
	invalidCredentials (49)	M	
	busy (51)	M	
	unavailable (52)	M	
	unwillingToPerform (53)	M	
	other (80)	M	
7.2	**Search**		ref. RFC1777:sec. 4.3
7.2.1	**Search Request**		

SECTION	FEATURE	STATUS	REMARKS
	Syntax		
	baseObject LDAPDN	M	ref. RFC1779
	scope	M	
	baseObject	M	
	singleLevel	M	
	wholeSubtree	M	
	derefAliases	M	
	neverDerefAliases	M	do not dereference aliases in searching or in locating the base object of the search
	sizeLimit INTEGER (0 … maxInt)	M	
	timeLimit INTEGER (0 … maxInt)	M	
	attrsOnly BOOLEAN	M	
	FALSE	M	both attribute types and values returned
	filter	M	
	and SET OF Filter	O	
	or SET OF Filter	O	
	not Filter	O	
	equalityMatch AttributeValueAssertion	O	
	substrings SubstringFilter	O	
	greaterOrEqual AttributeValueAssertion	O	
	lessOrEqual AttributeValueAssertion	O	
	present AttributeType	O	ref X.500
	approxMatch AttributeValueAssertion	O	
	attributes AttributeType	M	ref X.500
	Implementation of other aspects of protocol element by application providing LDAP repository search service	O	
7.2.2	**Search Response**		
	Implementation of entire protocol element by application providing LDAP repository search service	M	
	Syntax		
	objectName LDAPDN	M	ref. RFC1779
	attributes	M	
	AttributeType	M	ref X.500
	SET of AttributeValue	M	ref. RFC1778
	All values of multivalued attributes are returned	M	assumes requester has sufficient access permissions
	resultCode LDAPResult	M	ref. RFC1777:sec. 4
7.3	**Unbind**		ref RFC1777:sec. 4.2
	Implementation of full UnbindRequest by application providing LDAP repository search service	M	
8	**LDAP Repository Modify**	M	
8.1	**Bind**	M	ref. RFC1777:sec. 4.1
	Bind Request		
	Syntax	M	
	version INTEGER (2)	M	
	name LDAPDN	M	ref. RFC1779
	simpleauth OCTET STRING	M	
	Authenticated access	M	

SECTION	FEATURE	STATUS	REMARKS
	Bind Response	M	ref. 6.1.2
	Implementation of entire protocol element by application providing LDAP repository modify service	M	
	Minimum set of error codes recognized by clients	O	ref. RFC1777:sec. 4
	success (0)	M	
	operationsError (1)	M	
	protocolError (2)	M	
	authMethodNotSupported (7)	M	
	noSuchObject (32)	M	
	invalidDNSyntax (34)	M	
	inappropriateAuthentication (48)	M	
	invalidCredentials (49)	M	
	busy (51)	M	
	unavailable (52)	M	
	unwillingToPerform (53)	M	
	other (80)	M	
8.2	**Modify**	M	ref. RFC1777:sec. 4.4
8.2.1	**Modify Request**	M	
	Syntax	M	
	object LDAPDN	M	ref. RFC1779
	modification	M	
	operation	M	
	add	M	
	delete	M	
	modification	M	
	type AttributeType	M	ref X.500
	values SET of AttributeValue	M	ref. RFC1778
8.2.2	**Modify Response**	M	
	Implementation of entire protocol element by application providing LDAP repository modify service	M	
	LDAPResult	M	ref. RFC1777:sec. 4
8.3	**Add**	M	ref. RFC1777:sec. 4.5
8.3.1	**Add Request**	M	
	Implementation of entire protocol element by application providing LDAP repository modify service	M	
	Syntax	M	
	entry LDAPDN	M	
	attrs SEQUENCE	M	
	type AttributeType,	M	ref X.500
	values SET OF AttributeValue	M	ref. RFC1778
8.3.2	**Add Response**	M	
	Implementation of entire protocol element by application providing LDAP repository modify service	M	
	LDAPResult	M	ref. RFC1777:sec. 4
8.4	**Delete**	M	ref. RFC1777:sec. 4.6
8.4.1	**Delete Request**	M	
	LDAPDN	M	ref. RFC1779
8.4.2	**Delete Response**	M	
	Implementation of entire protocol element by application providing LDAP repository modify service	M	
	LDAPResult	M	ref. RFC1777:sec. 4
8.5	**Unbind**	M	ref RFC1777:sec. 4.2

SECTION	FEATURE	STATUS	REMARKS
	Implementation of full UnbindRequest by application providing LDAP repository modify service	M	
9	**Non-Standard Attribute Value Encodings**	M	To transfer v3 certificates & v2 CRLs,
	Syntax "Undefined"	M	ref. RFC1778:sec. 2.1
	Encode attribute value as if type OCTET STRING with the string value being the DER-encoded version of the value	M	
10	**Transport**	M	
	LDAPv2 transport over TCP	M	ref. RFC1777:sec. 3.1
	LDAPv2 transport over other reliable transports	O	
11	**Security Considerations**	M	
	CA requirements	M	
	Simple authentication	O	NOT RECOMMENDED
	Protection of password privacy	M	
	Physically secure networks	O	
	IPsec	O	
	SSH tunnel	O	
	TLS tunnel	O	
	SSL tunnel	O	
	Strong authentication	O	RECOMMENDED
	LDAP repository modify service access control	M	
	External CAs have access permission	O	
	Internal CAs have access permission	M	
	Access permission restricted to CA	M	
	CA can create	M	
	Entries of object class cRLDistributionPoint immediately subordinate to its own entry	M	
	CA can add	M	
	All PKI attributes for its own directory entry	M	
	All values of its PKI attributes	M	
	All attributes and all values of CRL Distribution Point entries	M	
	The attribute userCertificate and all its values issued by the CA to/from subscriber entries	M	
	CA can modify	M	
	All PKI attributes for its own directory entry	M	
	All values of its PKI attributes	M	
	Entries of object class cRLDistributionPoint immediately subordinate to its own entry	M	
	All attributes and all values of CRL Distribution Point entries	M	
	The attribute userCertificate and all its values issued by the CA to/from subscriber entries	M	
	CA can delete	M	
	All PKI attributes for its own directory entry	M	

SECTION	FEATURE	STATUS	REMARKS
	All values of its PKI attributes	M	
	Entries of object class cRLDistributionPoint immediately subordinate to its own entry	M	
	All attributes and all values of CRL Distribution Point entries	M	
	The attribute userCertificate and all its values issued by the CA to/from subscriber entries	M	
	Applications providing LDAP repository read service	O	
	Additional security measures	O	RECOMMENDED
	Applications providing LDAP repository search service	O	
	Additional security measures	O	RECOMMENDED
	Applications providing LDAP repository modify service	O	
	Additional security measures	O	RECOMMENDED

Document Point of Contact:

Defense Information Systems Agency
ATTN: JIEO-JEBBC (Gregor D. Scott)
Ft. Monmouth, NJ 07703-5613
USA
Voice: 732-427-6856
Fax: 732-532-0853
Email: scottg@ftm.disa.mil